DOCID:	4050MACIENTIAL
--------	----------------

SECURITY CLASSIFICATION

# NSA STAFF PROCESSING FORM

DDO EXREG CONTROL NUMBER		KCC CONTROL NUMBER		Z CONTROL NUMBER Z-054-98	
THRU		ACTI	APPROVAL	EXREG SUSPENSE	
CIA KRYPTOS Sculpture The Challenge and Resolution (U)		ACTION  X INFORMATION		ELEMENT SUSPENSE	
Z4 , Z2	3				

- **SUMMARY** (b) (3)-P.L. 86-36
- 1. (U) In response to your request we have put together a package chronologically outlining the events in our decryption (89%) of the CIA courtyard KRYPTOS sculpture. Also attached is a copy of the original memorandum to Adm. McConnell with attachments providing the cipher, the cryptography employed, and the respective decrypts.
- 2. (U) The initial examination of the cipher revealed that it was likely to consist of three cryptographically distinct sections. Basic computer diagnostic tools confirmed this hypothesis. Subsequent analysis and solution, however, did not require any compute power.
- 3. (C) Parts 1-3 were solved within two days of receiving the informal tasking from Chief, Z. Another day was spent on the final section and a decision was made to stop any further work. Given the suspected cryptography, the last section is too short to solve without diverting a great deal of effort from operational problems.

(b)(3)-P.L. 86-36

COORDINATION/APPROVAL SECURE SECURE OFFICE NAME AND DATE OFFICE NAME AND DATE PHONE PHONE Z09 7/22 5043s Drafter 4451s DATE PREPARED ORG PHONE (Secure) <sup>Z</sup>Approved for Release by NSA on 05-21-2013, FOIA Case # 61191. UNIO A0736 FEB 94 CLASSIFIED BY: NSA Class Guide 342-97 NSN: 7540-FM-001-5465 **Dated 29 May 1997** CONFIDENTIAL DECLASSIFY ON: X1, X5

Chronological history of NSA personnel and their involvement in the partial decryption of the KRYPTOS sculpture located in the CIA courtyard

- 1988 The CIA Fine Arts Commission approves James Sanborn's proposal.
- 1990 The artwork, titled *Kryptos*, is dedicated. A portion of this work of art consists of a classic Vigenere Square and 870 characters of cipher punched through two large copper sheets.
- 1991 While on a trip to the CIA headquarters, an informal group comprised mainly of Cryptanalysis interns, handwrites the cipher onto sheets of paper, and distributes it to any and all interested cryptanalysts back at NSA.
- $\bullet\,$  1992 Official challenge for solution is relayed through DCI at a Gold Bug award ceremony.
- 1992 Mr. \_\_\_\_\_\_\_ is the first person to decrypt a portion of the cipher. The cipher system used is a polyalphabetic substitution using eight alphabets. The decrypted text accounts for the last 373 characters from the first section of 436, but the initial 63 characters resist decryption. Because of this, analysts concede that four distinct sections are likely, with this being the second section. (b) (3)-P.L. 86-36
- 1992 Mr. \_\_\_\_\_\_ is the second person to successfully decrypt a portion of the cipher. That portion is the third section involving 337 characters and employing a transposition system using a matrix with dimensions 4 X 86.
- 1992 As the third successful cryptanalyst, Mr. successfully decrypts the initial 63 characters of the cipher, which is the first section. It also uses a polyalphabetic substitution, but with 10 alphabets.
- 1992 An informal document is produced detailing the solution of the three sections. These three sections comprise the first 773 characters out of 870 total, leaving the last 97 characters unresolved.
- 1993 A formal letter is sent to Adm. McConnell (DIRNSA) detailing the story, and is returned with a request that it be forwarded to Adm. Studeman at CIA.
- 1998 There is renewed interest from the CIA, with an eye towards a technical article for an internal publication.

DOCID: 4050989

DOCID: 4050989

DOCID: 4050989

UNITED STATES GOVERNMENT

TO ADMIRAL

STUDEMAN FOR INFO.

SUBJECT: CIA KRYPTOS Sculpture - Challenge and Resolution (FOUO)

INFORMATION MEMORANDUM

TO: DIR M
THRU: D/DIR 7, 7, EXEC/DIR DD, DDO M STORY.

- 1. (FOUO) The KRYPTOS sculpture, located at the entrance and in the courtyard of the new CIA headquarters, consists of a series of stone "pages" containing code which begins as International Morse and increases in complexity as the stonework extends into the courtyard. Inserted between these stone "pages" is a flat copper sheet engraved with letters and symbols the enciphered message that is the focus of this challenge.
- 2. (FOUO) In November, a cadre of cryptanalysts assigned to Z Group enthusiastically responded to the challenge. Within one month, three of the four cipher systems used to encrypt the sculpture's plain text had been diagnosed and completely exploited. The cryptographies employed for the encryption of these three parts involved two periodic polyalphabetic substitution ciphers and a keyed columnar transposition cipher. The exploitation of the sculpture's first three parts constitutes a readability of approximately 89%. The final 97 characters continue to elude solution.
- 3. (FOUO)— Attached, for your review, is a brief description of the employed cryptographies and the plain text derived from the three exploited portions of the KRYPTOS sculpture. If your schedule permits, we would be happy to present a 15-minute briefing on the KRYPTOS sculpture solution and introduce you to the cryptanalysts responsible for the success against this cipher.

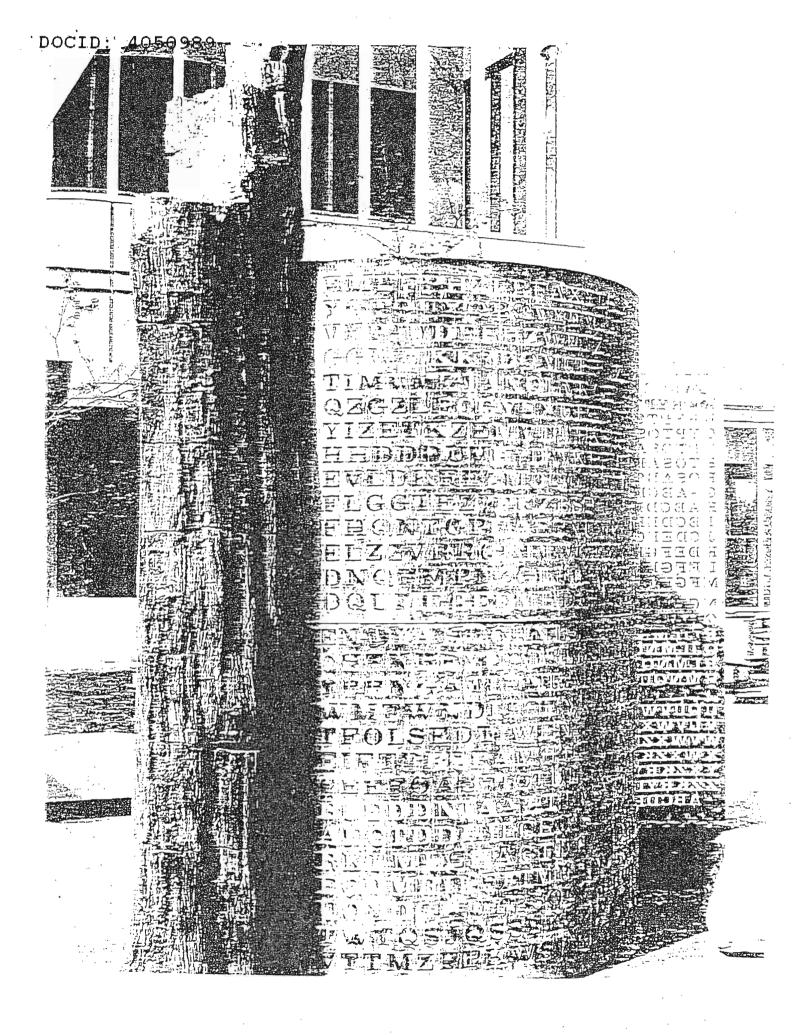
#### 3 Encls:

1. Copy of Sculpture Picture

2. Copy of Cipher

3. Description of Cryptographies

cc: Z4 Z43 (b) (3) - P.L. 86 - 36



#### THE KRYPTOS SCULPTURE CIPHER

```
EMUFPHZLRFAXYUSDJKZLDKRNSHGNFIVJ
YQTQUXQBQVYUVLLTREVJYQTMKYRDMFD
V F P J U D E E H Z W E T Z Y V G W E K K Q E T G F Q J N C E ·
G G W H K K 2 D Q M C P F Q Z D Q M M I A G P F X H Q R L G
T I M V M Z J A N Q L V K Q E D A G D V F R P J U N G E U N A
Q Z G Z L E C G Y U X U E E N J T B J L B Q C R T B J D F H J R R
YIZETKZEMVDUFKSJHKFWHKUWOLSZFTI
H H D D D U V H ? D W K B F U F P W N T D F I Y C U Q Z E R E
EVLDKFEZMOQQJLTTUGSYQPFEUNLAVIDX
F L G G T E Z ? F K Z B S F D Q V G O G I P U F X H H D R K F
F H O N T G P U A E C N U V P D J M Q C L Q U M U N E D F Q
ELZZVRRGKFFVOEEXBDMVPNFOXEZLGRE
D N Q F M P N Z G L F L P M R J Q Y A L M G N U V P D X V K P
D Q U M E B E D M H D A F M J G Z N T P L G E W J L L A E T G
ENDYAHROHNLSRHEOCPTEOIBIDYSHNAIA
C H T N R E Y U L D S L L S L L N O E S N O S M R W X M N E
T P R N G A T I H N R A R P E S L N N E L E B L P I I A C A E
W M T W N D I T E E N R A H C T E N E U D R E T N H A E O E
T F O L S E D T I W E N H A E I O Y T E Y Q H E E N C T A Y C R
EIFTBRSPAMHHEWENATAMATEGYEERLB
T E E F O A S F I O T U E T U A E O T O A R M A E E R T N R T I
BSEDDNIAAHTTMSTEWPIEROAGRIEWFEB
A E C T D D H I L C E I H S I T E G O E A O S D D R Y D L O R I T
R K L M L E H A G T D H A R D P N E O H M G F M F E U H E
E C D M R I P F E I M E H N L S S T T R T V D O H W ? O B K R
UOXOGHULBSOLIFBBWFLRVQQPRNGKSSO
TWTQSJQSSEKZZWATJKLUDIAWINFBNYP
V T T M Z F P K W G D K Z X T J C D I G K U H U A U E K C A R
```

## PART 1

Cryptography: Periodic Polyalphabetic Substitution employing

10 alphabets

Plain component: Keyword mixed sequence based on KRYPTOS Cipher component: Keyword mixed sequence based on KRYPTOS

Repeating Key: PALIMPSEST

Index letter: K

 P:
 K
 P
 P
 T
 O
 S
 A
 B
 C
 D
 E
 F
 G
 H
 I
 J
 L
 M
 N
 Q
 U
 V
 W
 X
 Z
 K
 R
 Y

 C1:
 P
 T
 O
 S
 A
 B
 C
 D
 E
 F
 G
 H
 I
 J
 L
 M
 N
 Q
 U
 V
 W
 X
 Z
 K
 R
 Y

 C3:
 L
 M
 N
 Q
 U
 V
 W
 X
 Z
 K
 R
 Y
 P
 T
 O
 S
 A
 B
 C
 D
 E
 F
 G
 H
 I
 J
 L
 W
 N
 Q
 U
 V
 W
 X
 Z
 K
 R
 Y
 P
 T
 O
 S
 A
 B
 C
 D
 E
 F</t

EMUFPHZLRF AXYUSDJKŽL DKRNSHGNFI VJYQTQUXQB BETWEENSUB TLESHADING ANDTHABSCE NCEOFLIGHT

QVYUVLLTRE VJYQTMKYRD MFD LIESTHENUA NCEOFIQLUS ION

(FOUO) Respaced and punctuated, it reads:

"BETWEEN SUBTLE SHADING AND THE ABSENCE OF LIGHT LIES THE NUANCE OF ILLUSION"

### PART 2

Cryptography: Periodic Polyalphabetic Substitution employing

8 alphabets

Plain component: Keyword mixed sequence based on KRYPTOS Cipher component: Keyword mixed sequence based on KRYPTOS

Repeating Key: ABSCISSA

Index letter: K

P: KRYPTOSABCDEFGHIJLMNQUVWXZ
C1: ABCDEFGHIJLMNQUVWXZKRYPTOS
C2: BCDEFGHIJLMNQUVWXZKRYPTOSA
C3: SABCDEFGHIJLMNQUVWXZKRYPTO
C4: CDEFGHIJLMNQUVWXZKRYPTOSAB
C5: IJLMNQUVWXZKRYPTOSAB
C6: SABCDEFGHIJLMNQUVWXZKRYPTO
C7: SABCDEFGHIJLMNQUVWXZKRYPTO
C8: ABCDEFGHIJLMNQUVWXZKRYPTO

VFPJUDEE HZWETZYV GWHKKOET GFQJNCEG GWHKK?DOM ITWASTOT ALLYINVI SIBLEHOW STHATPOS SIBLE?THE CPFQZDQM MIAGPFXH QRLGTIMV MZJANQLV KQEDAGDV YUSEDTHE EARTHSMA GNETICFI ELDXTHEI NFORMATI FRPJUNGE UNAQZGZL ECGYUXUE ENJTBJLB QCETBJDF ONWASGAT HEREDAND TRANSMIT TEDUNDER GROUNDTO HRRYIZET KZEMVDUF KSJHKFWH KUWQLSZF TIHHDDDU ANUNKNOW NLOCATIO NXDOESLA NGLEYKNO WABOUTTH VH?DWKBFU FPWNTDKI YCUQZERE EVLDKFEZ MOQQJLTT IS?THEYSH OULDITSB URIEDOUT THERESOM EWHEREXW UGSYOPFE UNLAVIDX FLGGTEZ?F KZESFDOV GOGIPUFX HOKNOWST HEEXACTL OCATION?O NLYWWTHI SWASHISL HHDRKFFH ONTGPUAE CNUVPDJM OCLOUMUN EDFOELZZ ASTMESSA GEXTHIRT YEIGHTDE GREESFIF TYSEVENM VRRGKFFV OEEXBDMV PNFOXEZL GREDNOFM PNZGLFLP INUTESSI XPOINTFI VESECOND SNORTHSE VENTYSEV

#### PART 3

Cryptography: Keyed Columnar transposition Matrix size: Incompletely filled 4 X 86

Specific key: KRYPTOS, numerically keyed and repeated 13 times

(first 12 columns listed below)

Route: Bottom to top

SLOWLYDESPARATLYSLOWLYTHEREMAINSOFPASSAGEDE ASREMOVEDWITHTREMBLINGHANDSIMADEATINYBREACH OLEALITTLEIINSERTEDTHECANDLEANDPEEREDINTHEH FLICKERBUTPRESENTLYDETAILSOFTHEROOMWITHINEM ' 1 1 1 2 1 0 BRISTHATENCUMBEREDTHELOWERPARTOFTHEDOORWAYW INTHEUPPERLEFTHANDCORNERANDTHENWIDENINGTHEH OTAIRESCAPINGFROMTHECHAMBERCAUSEDTHEFLAMETO ERGEDFROMTHEMISTXCANYOUSEEANYTHINGO 1 3

"SLOWLY DESPARATLY SLOWLY THE REMAINS OF PASSAGE DEBRIS THAT ENCUMBERED THE LOWER PART OF THE DOORWAY WAS REMOVED. WITH TREMBLING HANDS I MADE A TINY BREACH IN THE UPPER LEFT HAND CORNER, AND THEN, WIDENING THE HOLE A LITTLE, I INSERTED THE CANDLE AND PEERED IN. THE HOT AIR ESCAPING FROM THE CHAMBER CAUSED THE FLAME TO FLICKER, BUT PRESENTLY, DETAILS OF THE ROOM WITHIN EMERGED FROM THE MIST X CAN YOU SEE ANYTHING  $Q^{\prime\prime}$ .

Note: The above is a paraphrase from <u>The Tomb of Tut-Ankh-Amen</u> written by Mr. Howard Carter.